WHAT IS CLAIMED IS:

1. A method of screening for illegitimate requests to a computer application, comprising:

screening a request with a rule having at least one of an existential condition; a statistical condition; and a complex universal condition.

2. The method of claim 1 wherein screening with said rule is triggered by said request being of a certain type.

3. The method of claim 2 wherein said rule has a plurality of conditions and wherein said plurality of conditions are triggered by said request being of said certain type.

4. The method of claim 3 wherein said certain type is a certain type of universal resource identifier (URI).

5. The method of claim 1 wherein said existential condition requires that a specified number of elements of a given type exists in said request.

6. The method of claim 5 wherein said elements of a given type are one of Headers; Cookies; Universal Resource Identifier (URI) parameters; URI-encoded fields; multi-part encoded fields; Simple Object Access Protocol (SOAP) encoded elements.

7. The method of claim 1 wherein said existential condition requires that a specified number of elements of a given type with a given property exists in said request.

8. The method of claim 1 wherein said complex universal condition requires that a specified proportion of elements of a given type exist in said request.

9. The method of claim 1 wherein said statistical condition is based on a statistical measure of a property of elements of a certain type in a request.

10. The method of claim 9 wherein said property of elements of a certain type is one of a name or value of said elements of a certain type.

11. The method of claim 1 wherein said request is an hypertext transfer protocol (HTTP) request.

12. The method of claim 11 wherein said rule comprises conditions for one or more of the following parts of a request: Headers; Cookies; Methods; HTTP versions; Universal Resource Identifier (URI) parameters; URI-encoded fields; multi-part encoded fields; Simple Object Access Protocol (SOAP) elements.

13. The method of claim 3 wherein said body of said request follows Simple Object Access Protocol (SOAP).

14. A method of screening for illegitimate requests to a computer application, comprising:
screening a request with a rule having an existential condition.

15. A method of screening for illegitimate Hypertext Transfer Protocol (HTTP) requests to a computer application, comprising:
screening an HTTP request with a rule, said rule comprising a condition for at least one of the following parts of a request: Headers; Cookies; HTTP version indicators; Universal Resource Identifier (URI) parameters; URI-encoded fields; multi-part encoded fields; Simple Object Access Protocol (SOAP) elements; URI format.

16. The method of claim 15 wherein screening with said rule is triggered by a URI of said request being of a certain type.

17. The method of claim 15 further comprising, upon finding a request not meeting a condition, blocking said request.

18. The method of claim 15 further comprising, upon finding a request not meeting a condition, adding an entry to an event log.

19. The method of claim 15 further comprising, upon finding a request not meeting a condition, alerting.

20. A method of screening for illegitimate Hypertext Transfer Protocol (HTTP) requests to a computer application, comprising:

screening an HTTP request with a rule, said rule comprising a condition for fields or elements in a body of said request and a separate condition for Cookies of said request.

21. The method of claim 20 wherein said rule also comprises a condition for Universal Resource Identifier (URI) parameters of said request.

22. The method of claim 21 wherein said rule also comprises a condition for Methods of said request.

23. The method of claim 22 wherein said rule set also comprises a condition for an hyper-text transfer protocol (HTTP) version indicator of said request.

24. The method of claim 23 wherein said rule also comprises a condition for a URI format of said request.

25. The method of claim 24 wherein said rule also comprises a condition for a Header of said request.

26. A computer readable medium containing computer executable instructions which when loaded into a processor cause said processor to:

screen a request with a rule having one of an existential condition; a statistical condition; and a complex universal condition.

27. A computer readable medium containing computer executable instructions which when loaded into a processor cause said processor to:

screen an HTTP request with a rule, said rule comprising a condition for at least one of the following parts of a request: Headers; Cookies; HTTP version indicators; Universal Resource Identifier (URI) parameters; URI-encoded fields; multi-part encoded fields; Simple Object Access Protocol (SOAP) elements; URI format.

28. A screener comprising:

an input for receiving requests; and

means for screening a received request with a rule having one of an existential condition; a statistical condition; and a complex universal condition.

29. A screener comprising:

an input for receiving HTTP requests; and

means for screening an HTTP request with a rule, said rule comprising a condition for at least one of the following parts of a request: Headers; Cookies; HTTP version indicators; Universal Resource Identifier (URI) parameters; URI-encoded fields; multi-part encoded fields; Simple Object Access Protocol (SOAP) elements; URI format.

30. A method of screening for illegitimate Hypertext Transfer Protocol (HTTP) requests to a computer application, comprising:

screening an HTTP request with a rule, said rule comprising a condition for at least two of the following parts of a request: Headers; Cookies; Methods; HTTP versions; Universal Resource Identifier (URI) parameters; URI-encoded fields; multi-part encoded fields; Simple Object Access Protocol (SOAP) elements; URI format.